Manuel Höferlin
Member of the German Bundestag

Chairman Committee on the Digital Agenda

Digital Policy Spokesperson for the FDP-Bundestagsfraktion

Manuel Höferlin MdB, Platz der Republik 1, 11011 Berlin

Apple
Mr Tim Cook
One Apple Park Way
Cupertino, CA 95014
USA

Berlin, 16.08.2021

Manuel Höferlin MdB
Platz der Republik 1
11011 Berlin

Telefon: +49 30 227-78512
Telefax: +49 30 227-76512
manuel.hoeferlin@bundestag.de
http://manuel-hoeferlin.de

Dear Tim Cook,

I am writing to you today as Chairman of the Committee on the Digital Agenda at the German Bundestag, as I see a major threat posed by your plans for CSAM scanning.

To avoid any misunderstanding, let me be clear: sexual violence against children is a serious problem. That is why I expressly welcome Apple examining how it can be involved as a company in remedying this severe problem. The approach chosen by Apple however – namely CSAM scanning of end devices – is a dangerous one. Regardless of how noble your motives may be, you are embarking on a path that is very risky – not only for your own company. On the contrary, you would also be damaging one of the most important principles of the modern information society – secure and confidential communication. The price for this will most likely be paid not only by Apple, but by all of us. That is because CSAM represents the biggest opening of the floodgates for communication confidentiality since the birth of the internet. Every item of content scanned destroys some of the trust users place in not having their communications secretly monitored. The internet without information confidentiality would no longer represent great progress for civilization, but would instead be the largest instrument of surveillance in history.

That fact that you are now preparing to take this path with Apple is all the more surprising, given that in the past your company has often upheld the very principles of confidentiality and security. The trust that Apple has gradually built up with this stance could be lost overnight. Explanations of the strict limitation of the function will not change this, for as the EFF put it: "at the end of the day, even a thoroughly documented, carefully thought-out and narrowly-scoped backdoor is still a backdoor."

As much as I want to believe your assurances that you will reject all requests for further application of this function, such as the location of regime critics or surveillance of minorities, these lack credibility. In every country on Earth – even in my home country, despite our historical experiences – political forces continue to coalesce for whom confidential communication and encryption are a thorn in their side, and who are engaged in ongoing efforts to replace freedom with surveillance. For people who unlike us are not lucky enough to live in Western democracies, this can in the worst-case scenario mean a genuine threat to their lives.

In concrete terms for Apple, this means that in future you will need to decide whether to keep your promise to limit the functionality, or continue doing business in markets such as China, Russia or other authoritarian states. Such requests will come from these countries, too, under the pretext of fighting terror or other ostensibly lofty goals – that much is certain. The fact that these requests mask very different objectives to some extent is just as certain. That is why my urgent appeal to you is that you abandon your plans for CSAM scanning. This would not only save your own company from many foreseeable problems, but would also protect the Achilles' heel of the modern information society! Please stay on the side of those who defend civilization's achievement of a free internet!

Yours sincerely

Manuel Höferlin MdB